Innominate mGuard

Version 8.1.5 - Release Notes

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin, Germany
Tel.: +49 30 921028-0
e-mail: contact@innominate.com
http://www.innominate.com/

Innominate Document Number: RN208152115-065

Vertical bars to the left mark significant changes in firmware 8.1.5 in comparison to the release notes for firmware version 8.1.4

1 Product Description

1.1 Supported Hardware

The firmware can be operated on the following hardware platforms:

- mGuard core²
- mGuard pci² SD
- mGuard pcie² SD
- mGuard delta²
- mGuard rs2000
- mGuard rs4000
- mGuard industrial RS
- mGuard smart²
- mGuard smart
- mGuard core
- mGuard pci
- mGuard blade
- EAGLE mGuard / mGuard industrial
- mGuard delta
- FL MGUARD GT/GT
- mGuard rs2000 4TX/3G
- mGuard rs4000 4TX/3G/TX VPN
- mGuard rs2000 5TX/TX
- mGuard rs4000 4TX/TX
- mGuard rs4000 TX/TX PA
- mGuard centerport
- mGuard centerport2

For detailed information about these platforms please see the technical data sheets, which are offered for download at http://www.innominate.com/ .

1.2 Software Features

The firmware provides the functionality of a network firewall with support for VPN connections (license controlled) and other services. The complete features are listed and described in detail within the user manual, which can be downloaded from http://www.innominate.com/ .

1.3 Changes Since Previous Release

- This release fixes NTP security issue CVE-2014-9295 which allows remote code execution with reduced privileges. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20150120_001_en.pdf
- It fixes communication failure due to dynamically opened ports under certain conditions not being allowed by the OPC Inspector
- It improves data transfer speed through VPN on centerport class devices

1.4 Firmware installation and update

- The firmware version 8.x requires a Major Upgrade License for devices manufactured before 2013.
- The Configuration Pull mechanism must be disabled during the time of the update.
- The “CRL checking” feature (verifying the validity of X.509 certificates with the help of a Certificate Revocation List) must be disabled.

Please also refer to
http://www.innominate.com/data/downloads/manuals/update-recovery-flash-guide-v8.pdf

1.5 Important update information (updating to 8.1.5)

The devices listed in the following table and equipped with the given firmware version can be updated to firmware version 8.1.5.

	mGuard industrial RS	mGuard smart	mGuard core	mGuard pci	mGuard blade	EAGLE mGuard / mGuard industrial	mGuard delta	mGuard smart²	mGuard core²	mGuard pci(e)² SD	mGuard delta²	mGuard rs2000/4000	FL MGUARD GT/GT	mGuard rs2000/4000 4TX/3G	mGuard centerport	mGuard centerport 2
7.0.x													√			
7.1.x,													√			
7.2.x								√					√		√	
7.3.1								√	√				√		√	
7.4.x								√	√		√	√	√		√	
7.5.0								√	√	√	√	√	√		√	
7.6.x								√	√	√	√	√	√		√	
8.0.0														√		
8.0.1	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
8.0.2	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
8.1.0	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
8.1.1	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
8.1.2	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
8.1.3	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
8.1.4	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

1.6 Important installation information (flashing with 8.1.5)

1.6.1 Platform MGUARD2

This platform includes the following devices:

- mGuard smart²
- mGuard core²
- mGuard pci² SD
- mGuard pcie² SD
- mGuard delta²
- mGuard rs2000
- mGuard rs4000
- mGuard rs2000 4TX/3G
- mGuard rs4000 4TX/3G/TX VPN
- mGuard rs2000 5TX/TX
- mGuard rs4000 4TX/TX
- mGuard rs4000 TX/TX PA

The firmware files for this platform are called **ubifs.img.mpc83xx.p7s** and **install-ubi.mpc83xx.p7s**.

1.6.2 Platform FL MGUARD GT/GT

The firmware files for this platform are called **jffs2.img.mpc83xx.p7s** and **install.mpc83xx.p7s**.

1.6.3 Platform Intel IXP4xx

This platform includes the following devices:

- mGuard industrial RS
- mGuard smart
- mGuard core
- mGuard pci
- mGuard blade
- EAGLE mGuard / mGuard industrial
- mGuard delta

The firmware files for this platform are called **jffs2.img.p7s** and **install.p7s**.

1.6.4 Platform Centerport and Centerport2

The firmware files for this platform are called **firmware.img.x86_64.p7s** and **install.x86_64.p7s**.

1.6.5 Obtaining the firmware and update files

As of release 3.0.0 customers must register before downloading the firmware files. Please refer to

http://www.innominate.com/register_software
http://www.innominate.de/register_software.

After registration user and password information is sent. Please note that the update server is operating using the “HTTPS” protocol.

2 Version History

This chapter lists the changes between former versions of the mGuard firmware.

2.1 Changes made between 8.1.3 and 8.1.4

This patch release supports three new hardware variants, fixes two security issues and some minor functionality issues:

- The new hardware devices mGuard rs2000 5TX/TX, rs4000 4TX/TX and rs4000 TX/TX PA are supported with this release.
- This release fixes the OpenVPN security issue CVE-2014-8104 which allows to attack the mGuard IPSec TCP encapsulation. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20141217_002_en.pdf
- It also fixes a privilege escalation issue for the admin user (CVE-2014-9193). Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20141217_001_en.pdf
- It incorporates the fix for the PPPD integer overflow issue tracked as CVE-2014-3158, even though the issue cannot be used to attack the mGuard.
- The recovery procedure on 3G based devices now correctly sets the local IP to 192.168.1.1.
- Remote VPN masquerading by the internal mGuard IP is now fully supported.
- This release improves the memory management for many VPN connections on legacy devices.
- It improves the storage of the SNMPv3 credentials.
- The reliability of devices with a full filesystem and during a sudden power interruption got improved in this release.

2.2 Changes made between 8.1.2 and 8.1.3

This patch release fixes a compatibility issue with the Innominate mGuard device manager (mdm) version 1.4:

- A device configuration created with mdm for devices with firmware version 8.1.0, 8.1.1 or 8.1.2 cannot be applied if the device version in mdm is set to 7.4 or below.

2.3 Changes made between 8.1.1 and 8.1.2

This patch release contains bug fixes observed in version 8.1.0 and 8.1.1:

- It re-enables local 1:1 NAT in a Hub&Spoke VPN scenario.
- It increases the partition size of centerport devices.
- It fixes and re-enables the redundancy feature (memory issue and accessability after interface reconfiguration)
- It fixes issues with importing and saving configuration profiles.
- The following Release-Notes issues got fixed:
  - Issue “Expected conntrack entries are not deleted” (Ref. 12227)
  - Issue “The DMZ port of the centerport2 device is not usable” (Ref. 12318)
  - Issue “Serial console over USB not working on smart²” (Ref. 11995)

2.4 Changes made between 8.1.0 and 8.1.1

This release fixes the OpenSSL security issue CVE-2014-0224. The affected mGuard firmware versions are 8.0.0, 8.0.1, 8.0.2 and 8.1.0.

It is strongly recommended to update all devices operating with the firmware version 8.0.0, 8.0.1, 8.0.2 or 8.1.0.

After the update the device should be rebooted.

Please also see the Innominate Security Advisory at:

http://www.innominate.com/data/downloads/software/innominate_security_advisory_20140606_001_en.pdf

2.5 Changes made between 8.0.2 and 8.1.0

- The new mGuard OPC Inspector enables firewall filtering and NAT on OPC Classic traffic.
- This release supports several different Dynamic DNS providers and configurable dyndns.com-compatible providers.
- It supports mapping multiple internal network segments into a single VPN channel using 1:1 NAT.
- The list of currently logged in Firewall users is now updated dynamically in the Web UI. Changes to Firewall Rules affecting logged in users are now applied immediately without the need for users to log in again.
- Firewall Rule Records and VPN Connections can now be triggered by up to three external switches, the command line interface, the Web interface or a CGI URL.
- Supervising VPN Connections and Firewall Rule Records using a hardware output can now be configured independently of a controlling switch or button.
- The User-Firewall and switchable Firewall Rule Records are now usable inside VPN connections.
- This release supports querying different states via the CGI interface like CIFS Integrity Monitoring results, Firewall Rule Record states, VPN states, ECS and Modem states.
- The CGI interface now also allows to perform actions like starting and stopping CIFS scans or Firewall Rule Records, as well as logging out Firewall users.

2.6 Changes made between 8.0.1 and 8.0.2

- This release fixes the OpenSSL security issue CVE-2014-0160 known as Heartbleed vulnerability. The affected mGuard firmware versions are 8.0.0 and 8.0.1. All other mGuard software releases are not affected.
- Please also see our Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20140411_001_en.pdf

2.7 Changes made between 7.6.2 and 8.0.1

- A short abstract of the software features supported on the new mGuard rs2000 4TX/3G and mGuard rs4000 4TX/3G/TX VPN devices:
  - Mobile Network connection (2G/3G technology) for Europe
  - Sending and receiving SMS
  - Positioning System (GPS).

  - Configuration of the managed switch
  - Multicast support
  - Additional Network port (DMZ) (rs4000 4TX/3G/TX VPN only)
- This release supports sending E-Mails triggered by configurable events.
- It extends the options to temporarily enable VPN connections as there are SMS, command-line and Web UI.
- It provides an RFC2217 compliant TCP to Serial line service.
- System events are now updated automatically in the Web UI without the need to refresh the page.
- It improves the CIFS-IM and CIFS-AV feature in combination with Windows 95/98 hosts.
- It fixes the QoS feature.

2.8 Changes made between 7.6.1 and 7.6.2

- This release fixes TCP encapsulated VPN connections in configurations where the redundancy feature is enabled.
- ARP replies for VPN remote networks on the external interface in multiple stealth mode are suppressed with this release.
- All IPSec SAs are now deleted in case of shutting down a connection because of a dead peer detection (DPD).
- This release improves reestablishment of VPN connections over unstable lines like an overloaded WLAN.
- It also fixes an issue that broke the CIFS feature during an update on mGuard smart, pci, blade, delta and EAGLE mGuard.
- A rare, unexpected reboot under heavy load is fixed in this release.
- Management access via the internal IP through a VPN tunnel works correctly now when the VPN network is a subnet of the local network.
- TCP Encapsulation and any other HTTP traffic initiated by the mGuard using a Sophos Proxy with NTLM authentication is now supported.
- This release fixes failures of Hub&Spoke triggered by configuration changes of the involved VPN connections.
- Syslog messages to a remote Syslog server are now sent through the appropriate VPN connection, even with local 1:1 NAT enabled inside the VPN tunnel.

2.9 Changes made between 7.6.0 and 7.6.1

- Innominate mGuard blade devices did not function properly with the Innominate mGuard Firmware version 7.6.0. After an update the previous configuration was lost on blade devices. The blade controller did not show the blade menu in the web interface anymore. Affected devices are:
  - mGuard blade /533 // HW-104050
  - mGuard blade /266 // HW-104020
  - mGuard bladebase // HW-104500
  - mGuard bladepack /533 // HW-104850
  - mGuard bladepack /266 // HW-104820

  This is fixed in this release.

2.10 Changes made between 7.5.0 and 7.6.0

- The DPD (Dead-Peer-Detection) behavior and the connection-management of the VPN IPsec service have been improved.

- It now supports TPM (Trusted Platform Module) encrypted profiles and ECS storage on the platforms mGuard rs2000, mGuard rs4000, mGuard pci² SD, mGuard pcie² SD and mGuard centerport.
- The global Firewall selector now allows to permit ping (ICMP echo) next to allowing or rejecting all traffic.

2.11 Changes made between 7.4.1 and 7.5.0

- Redundancy in stealth mode “multiple clients” is supported with this release.
- A system-wide configuration option controls the conntrack table flush during firewall reconfiguration.
- The new setting Redundancy Failover Latency configures a grace period that must elapse, before a connectivity failure will take effect.
- It is now possible to configure a NAS identifier for RADIUS authentication.
- The FAULT LED and contact can now be configured to also supervise the configured temperature range and the redundancy connectivity check state.
- A NET-BIOS name can be configured to import network shares exported by Microsoft Windows 98 machines.
- Configuration profiles that can't be applied are now rejected during upload with an appropriate error message.
- Scanning of Microsoft Windows 98 shares was improved.
- Added function for renewing RSA keys via GUI and command line.
- RSA keys newly generated when flashing or using the new function have a modulus of 2048bit.
- The IP for incoming VPN connections can be configured now.

2.12 Changes made between 7.4.0 and 7.4.1

- It fixes an issue with “IKE Fragmentation” which could cause failure (hang/restart) of the IPsec VPN subsystem.
- It fixes memory leaks and connection stalls triggered by remote peers being located behind NAT gateways.
- It fixes an issue with administrative access to the mGuard via VPN failing if VPN is activated via CMD button or switch.
- It fixes the issue “Remote access through VPN” with administrative access to the mGuard via VPN failing if the default route is via VPN.
- It fixes an issue with a VPN tunnel not being re-established after reboot if the CMD switch is still “enabled”.
- It fixes an issue with very large numbers of port forwarding rules (>1000).
- It fixes the issue “Many IPsec SAs established”: IPsec SAs are no longer unnecessarily generated with DynDNS monitoring enabled.
- It re-enables the “user” account to activate VPN tunnels using “nph-vpn.cgi” interface.
- It supports ICMP echo requests to the internal administrative IP of the mGuard through VPN tunnels with NAT settings enabled.
- It supports use of CA certificates with BMPSTRING subjects.
- It supports fast DHCP renewal after link loss on the external interface in Router/DHCP mode.
- It improves compatibility of NTLM proxy authentication with MS Forefront
- It improves detection of topology changes in autodetect Stealth Mode.

2.13 Changes made between 7.3.1 and 7.4.0

- Version 7.4.0 supports the new hardware platforms mGuard rs2000 and mGuard rs4000.
- It eases the password rollover for a redundancy pair.
- It allows to configure session limits for authenticated SSH sessions.
- The firewall in version 7.4.0 allows to filter or forward GRE protocol packets.
- It supports remote masquerading and improves the possible combinations of masquerading and 1:1 NAT through VPN connections.
- NAT-T handling with VPN redundancy is improved.
- The design of the GUI has been improved in this version.
- Enabling and disabling TCP encapsulated VPN connections by the CMD contact has been fixed.
- Version 7.4.0 fixes authentication failures of T-Online DSL connections with account numbers less than 24 digits which require the '#' sign.

2.14 Changes made between 7.2.1 and 7.3.1

(Version 7.3.0 was released for a limited set of platforms.)

- Devices with less than 64 MB of RAM are not supported anymore by firmware version 7.3.1.
- Version 7.3.1 revives the license controlled firewall redundancy feature for the network mode “Router”. For the mGuard centerport it even supports an improved fail-over switching time of one second at most (optionally longer).
- It adds the license controlled VPN redundancy feature.
- It adds support for the SHA2 algorithms SHA-256, SHA-384, and SHA-512 for VPN connections, see also issues “Interoperability of SHA2 and IPsec”.
- It adds support for preference lists of algorithms to use for VPN connections.
- It allows to configure a traffic limit for the lifetime of IPsec Security Associations (IPsec SAs).
- It adds the feature to use RADIUS servers for authentication of users of the web interface and the Command Line Interface. The RADIUS servers may optionally be reachable through VPN channels.
- It allows to perform the online downloads of future firmware versions through a VPN channel.
- It adds a configuration option which allows it to download CRLs through VPN channels.
- It improves the logging of administrative sessions and important administrative actions.
- It adds a configuration option which allows to disable the ARP replies at the external interface for 1:1 NAT scenarios.
- It adds optional Hub & Spoke support between a SEC-Stick connection and VPN connections.
- It fixes the issue “Remote access ports not configurable for access via VPN”.
- It fixes the issue “Features not supported with firmware version 7.2.1”.
- It avoids unexpected configuration changes of the blade controller.
- The changing of the password for the CIFS AV Scan Connector no longer requires a reboot.
- It improves use of several L2TP connections at the same time.
- It improves establishment of TCP encapsulated VPN connections after reboot.
- It improves the logging for TCP encapsulated VPN connections.
- It raises the limit for the number of port-forwardings per SEC-Stick connection.

- It fixes logging of SEC-Stick access.
- It adds support for enabling persistent logging for TCP encapsulated VPN connections.
- It closes the potential security issues CVE-2010-3301, CVE-2010-2240, CVE-2010-0405, CVE-2010-3301, CVE-2010-4258, CVE-2010-3848, CVE-2010-3849, and CVE-2010-3850. None of which affects the mGuard in a way which requires a user to take action immediately.

2.15 Changes made between 7.2.0 and 7.2.1

- Version 7.2.1 adds support for a new hardware revision of the EAGLE mGuard product

3 Identified Issues and Workarounds

Issue “PSK + Aggressive Mode is insecure” (Ref. 12168)

	Description
Synopsis	The IKE Aggressive Mode protocol has known flaws in combination with PSK. This is a protocol weakness and not an mGuard weakness.
Symptom	VPN Connections may be decrypted and modified by unauthorized entities.
Workaround / Action	Avoid using PSK+Aggressive Mode. The use of certificates with Main Mode is strongly recommended.

Issue “PSK + Aggressive mode with DH groups” (Ref. 12051)

	Description
Synopsis	Aggressive Mode VPN connection initiators behind the same NAT gateway must use the same, fixed DH group. If there are several Aggressive Mode connections to which the mGuard is the responder, it will be necessary to set the DH group on the responder to "all algorithms". If a fixed DH group is used on the responder, it must be the same group for all Aggressive Mode connections.
Symptom	Aggressive Mode connections with different DH groups not matching the restrictions above are not established.
Workaround / Action	The use of certificates with Main Mode is strongly recommended.

Issue “Updating a redundancy pair from version 7.x does not work” (Ref. 12205)

	Description
Synopsis	When updating both devices at the same time the standby device performs the update whereas the master device does not.
Symptom	The update of the master device fails and it remains at the old version.
Workaround / Action	Given that only the device currently on standby can be updated, proceed to update the standby device first. After the update is finished and the device is up, reboot the active device (running the old version). This allows the updated device to become active. Then proceed to update the (now on standby) device.

Issue “Redundancy internal link detection devices with switch” (Ref.10959)

	Description
Synopsis	The setting “Ethernet link detection only” for the redundancy connectivity checks of the internal interface on devices with internal switch always reports an established link even without connectivity.
Symptom	A link failure on one of the switch ports LAN1 - LAN4 is not detected.
Workaround / Action	Use ICMP echo request targets for connectivity checks of the internal interface on devices with internal switch.

Issue “VLAN in stealth mode with redundancy enabled” (Ref.10425)

	Description
Synopsis	When operating a device in stealth mode with redundancy and VLAN enabled may unexpectedly block some traffic.
Symptom	Some VLAN traffic will be blocked unexpectedly.
Workaround / Action	None.

Issue “Flow control does not send PAUSE frames” (Ref.10986)

	Description
Synopsis	In case of enabled and negotiated Flow-Control, the device will not send PAUSE frames in case of congestion.
Symptom	The device will drop more packets as expected even with Flow-Control enabled on this port.
Workaround / Action	None.

Issue “Radius authentication over VPN with redundancy” (Ref.10913)

	Description
Synopsis	Radius authentication over VPN from the passive device in a redundancy setup over the VPN connection of the active device does not work.
Symptom	Login with radius authentication on a passive device in a redundancy setup does not work if the radius server is only reachable via a VPN tunnel of the active device.
Workaround / Action	None.

Issue “Mounting Microsoft Windows 98 shares” (Ref.9762)

	Description
Synopsis	A once correctly configured NetBIOS name (RFC1001) for Microsoft Windows 98 shares will stay active until a reboot.

Symptom	When mounting several shares from the same Microsoft Windows 98 host all shares can be mounted successfully as long as the correct NetBIOS name was supplied at least once for at least one share.
Workaround / Action	Reboot the mGuard after reconfiguration

Issue “Scanning of Windows shares may fail” (Ref.9651)

	Description
Synopsis	The scan report may not be created when the report-share is a subdirectory of the share to be scanned.
Symptom	The scan report “integrity-check-log.txt” is not updated or created. The check finishes with the following status message: *Last check aborted with error code 1. The process failed due to an unforeseen condition, please consult the logs.* This effect depends on the version of the Microsoft Windows operating system.
Workaround / Action	Use a different share for the report/ database, which is not a subdirectory of the share to be scanned on the Windows host.

Issue “CIFS IM pattern matching is now case insensitive” (Ref.9432)

	Description
Synopsis	The filename pattern matching functionality of the CIFS Integrity Monitoring is now case-insensitive.
Symptom	Filenames containing uppercase letters in their extension are now recognized and will be shown as unexpected files after an update from version 7.4.1 or below.
Workaround / Action	Regenerate the CIFS IM database.

Issue “ICMP failure with transport VPN in Stealth Mode with SNMP”

	Description
Synopsis	ICMP echo requests are not answered through a transport mode VPN connection if the device is in Stealth Mode and SNMP is activated
Symptom	From a remote peer a client protected by an mGuard shall be pinged through a transport mode VPN. The tunnel is up and other traffic succeeds but ICMP echo requests are not answered. This problem only occurs if SNMP is enabled on the mGuard.
Workaround / Action	None.

Issue “Administrative Access From Moved Client in Single Stealth”

	Description
Synopsis	In single stealth auto detect and static modes the client cannot access the mGuard if the client was moved to the extern (unprotected) side.
Symptom	In single stealth mode the mGuard records the client computer's IP and MAC address at the internal (protected) interface and uses it to direct traffic to the client. If the client computer is moved to the extern (unprotected) side and tries to communicate with the mGuard (even using the management IP address) communication is not possible, as the mGuard still tries to direct the traffic to the internal (protected) side.
Workaround / Action	Do connect another client computer to the internal (protected) interface so that mGuard can learn new addresses for IP and MAC or reboot the mGuard.

Issue “Particular self signed certificates not accepted as HTTPS client certificates”

	Description
Synopsis	Self signed certificates can be configured as acceptable certificates “per definition” if they are used by browsers to authenticate administrative access to the mGuard's GUI. Nonetheless such certificates are rejected if the command “`openssl verify -CAfile cert.crt -purpose sslclient cert.crt`” would verify them as invalid.
Symptom	Access is rejected by the mGuard, although the configured self-signed certificate is used by the browser.
Workaround / Action	Create a different certificate having an appropriate or no key usage extension. For hints about which key usage extensions are missing, please check the output of the command “`openssl verify -issuer_checks -CAfile cert.crt -purpose sslclient cert.crt`“

Issue “Changed Flood Protection Settings delayed for VPN connections”

	Description
Synopsis	When settings are changed within the menu “Network Security / DOS Protection”, these do not become effective for VPN connections immediately, while they do for the incoming and outgoing

	firewall. The changed settings become effective as soon as VPN connections are restarted.
Symptom	Changed flood protection settings have no effect for established VPN connections.
Workaround / Action	Restart the VPN connections or reboot the device.

Issue “Reconfiguration of VLAN ID not noticed by DHCP server”

	Description
Synopsis	If an mGuard is operated in *stealth mode* with a *DHCP* server on the *internal interface,* a reconfiguration of the VLAN ID is not noticed by the DHCP server. The DHCP server continues to use the old VLAN ID.
Symptom	After reconfiguration of the VLAN ID the internal DHCP server does no longer respond to requests from clients.
Workaround / Action	Please disable and re-enable the DHCP server or restart the mGuard after such a configuration change.

Issue “Identical VPN connections just with different machine cert do no work”

	Description
Synopsis	If several VPN connections (at least two) are configured to use the same settings except for the local machine certificate and if they use a CA-certificate to authenticate remote sites the mGuard might assign incoming connections the wrong way.
Symptom	All incoming VPN connections are always assigned to the first VPN connection which matches the credentials provided by the peer. Thus the mGuard always uses the first machine certificate to authenticate itself to the remote side – even if the remote side is configured to accept the other machine certificate only. The connection attempt fails.
Workaround / Action	Please distinguish your remote sites by issuing certificates from a different (sub-)certification authority for them. A different (sub-)CA-certificate is required per VPN connection. Sites to connect to the same connection must use certificates issued by the same CA-Certificate.

Issue “Transport mode VPN with %any as gateway not supported in stealth mode”

	Description
Synopsis	For any stealth mode operation the

	mGuard does not support the a VPN connection in transport mode with %any as gateway and CA authentication of several peers at once. Such scenarios do work only if just one peer connects.
Symptom	If more than one peer establishes a connection to the same transport mode VPN connection of the mGuard operating in stealth mode then packets might not get through the channel.
Workaround / action	Please use tunnel mode VPN connections.

Issue “Remote access ports not configurable for stealth(multi) with VLAN”

	Description
Synopsis	If an mGuard is operated in network mode “stealth” with “multiple clients” and has a VLAN ID configured for its management IP then HTTPS/SSH/SNMP remote access to that IP does only work if default ports are configured (443/22/161).
Symptom	If other than the default remote access ports are configured, no connection can be established to the management IP on those ports. The mGuard does not respond.
Workaround / Action	Do not change the default ports.

Issue “netadmin cannot perform a test download for the Configuration Pull” (Ref.7540)

	Description
Synopsis	Through the GUI, the user “netadmin” cannot perform a test download of the configuration profile stored on a central HTTPS server.
Symptom	Even if the configuration is correct, “netadmin” will always see that the test download fails, for example with the message “The requested URL returned error: 401”.
Workaround / Action	None

Issue “Interoperability of SHA2 and IPsec” (Ref.8510)

	Description
Synopsis	When configured to use a SHA2 (SHA-256, SHA-384, and SHA-512) algorithm for use with IPsec the mGuard is not interoperable with some other vendors’ implementations of IPsec in combination with SHA2.
Symptom	If the other VPN appliance also supports SHA2 and is correctly configured the ISAKMP SA and the IPsec SA are

	established. But no traffic is passed through the VPN tunnel. The mGuard rejects to decrypt traffic from the peer and vice versa. The reason is that the mGuard and the peer do not agree about the number of bits to which to reduce the output of the SHA2 algorithms.
Workaround / Action	Please use an mGuard at both sides or do not use SHA2 for IPsec if interoperability with the particular vendors is required.

Issue “Segmented large OPC messages may be not accepted by Sanity Check" (Ref. 14054)

	Description
Synopsis	If the length of OPC messages exceeds the TCP Window Size between OPC server and OPC client, communication may stop before the full message was sent and could be processed by the OPC Inspector with Sanity Check.
Symptom	Affected OPC connections get stuck.
Workaround / Action	If possible, enlarge the TCP window size between OPC server and OPC client to fit all OPC messages or disable OPC Sanity Check. Since the TCP window size, scaling and configuration depends on the Microsoft Windows version used, no general recommendation can be provided. Please refer to Microsoft TechNet or Knowledge Base.

4 Known Restrictions

- The Safari browser needs to have all sub-CA certificates installed in its trust store if they are used to authenticate for administrative access to the mGuard via X.509 certificate.
- The same browser instance cannot be used to administrate the mGuard with X.509 authentication and to login into the mGuard's user firewall at the same time.
- Configuration of the mGuard via its web interface, via its Command Line Interface (shell access), and via SNMP must not happen concurrently. Concurrent configuration operations via different access methods may cause unexpected results.
- The external DHCP server of the mGuard cannot be used in multi stealth mode if a VLAN ID is assigned to the management IP.

5 Documentation Updates / Errata

- currently none